REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks.

By this amendment, claims 1, 12 and 19 are amended. No new matter has been added. Accordingly, claims 1-10 and 12-19 are pending in the present application.

STATEMENT OF INTERVIEW

The courtesy extended by Examiner Su to the Applicants' representative at the interview on July 7, 2010, is greatly appreciated.

In the Office Action dated February 5, 2010, claims 1-5, 12, 13, 15, 16 and 19 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Hopkins et al. (U.S. Patent Application Publication No. 2005/0190912 A1, hereinafter "Hopkin")

At the interview, Applicants' representative first explained the differences between the present invention and the Hopkins reference.

Applicants would like to explain exemplary embodiments in more detail here with reference to the specification. According to Applicants' exemplary embodiments, a method of generating a private key d for a public-key cryptography method using a secure electronic object device comprises two separate calculation steps:

Step A

- 1) calculating pairs of prime numbers (p,q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of the pair (e,l) in which e is the public exponent and l is the length of the key of the cryptography method, l also being the length of the modulus N of said method,

- 2) storing the pairs or values thus obtained;

Step B

- calculating the key d from the results of step A and knowledge of the pair (e,l).
-

See Applicants' published specification, US Pub No. 2005/0226411, paragraphs 0052-0056. The secure electronic object includes programs for implementing steps A, and B, wherein steps A and B are executed separately in terms of time. See Applicants' published specification: paragraph 0088. The calculation of step A may be carried out by the secure electronic object itself at any given instant which does not disturb the user of this secure electronic object. See Applicants' published specification: paragraph 0106. During use of the card, if a private key is requested, the calculation of step B) is carried out rapidly by the secure electronic object. See Applicants' published specification: paragraph 0108. As a result, generation of a private key can be carried out by the secure electronic object itself with a 10-fold gain in execution time compared to the conventional key generation methods. See Applicants' published specification: paragraph 0110.

During the interview, Applicants' representative explained the significance of storing the prime numbers (p,q) calculated during step A, to be later used in Step B, for verification of the prime numbers (p,q).

Examiner Su suggested amending claim 1 to clarify the order of the steps of storing and verifying the prime numbers.

Accordingly, claim 1 is amended, for clarification, to recite, in Step A, <u>prior to a secure electronic object is requested to generate a private key,</u> calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this

calculation being independent of knowledge of a pair of values (e, l) in which e is the public exponent and l is the length of the key of the cryptography method.

Claim 1 further recite, in Step B, in response to the secure electronic object being requested to generate a private key, retrieving a pair of prime numbers (p, q), or a value representative of said pair of prime numbers, stored in step A;

subsequent to the step of storing the calculated pairs of prime numbers or values and the step of retrieving the pair of prime numbers (p, q), or the value representative of said pair of prime numbers, verifying the following conditions for said pair of prime numbers:

(i) p-1 and q-1 are prime numbers with the obtained value for e and

(ii) N=p*q is an integer of given length l.

Hopkins does not disclose the above-recited features of claim 1. To the extent that Hopkins discloses verification of prime numbers, it is in connection with the initial computation of a set of cryptographic parameters. This process occurs prior to storage of the set in memory. See the flowchart of Fig. 6 in which the computation step 122 is before the storage step 124.

Thereafter, Hopkins merely discloses that a determination is made at step 128 whether one of the pre-computed sets of cryptographic parameters has the characteristics specified in a request. Therefore, Hopkins does not explicitly disclose obtaining values for e and l and verifying the conditions (i) and (ii) for a pair of the prime numbers subsequent to the step of storing the calculated pairs of prime numbers or values and the step of retrieving the pair of prime numbers (p, q), or the value representative of said pair of prime numbers, as described in claim 1.

In addition, Hopkins does not inherently disclose verifying the conditions (i) and (ii) for a pair of the prime numbers subsequent to the step of storing the calculated pairs of prime numbers or values and the step of retrieving the pair of prime numbers (p, q), or the value representative of said pair of prime numbers, as described in claim 1.

. Hopkins discloses that the pre-computed sets of cryptographic parameters are generated and stored in association with different values of public exponent e and length l. Therefore, it is likely that the choice of a pre-computed set of cryptographic parameters is made based on the public exponent e and length L that is used to generate the pre-computed sets of cryptographic parameters. In that case, the system as disclosed in Hopkins would not need to additionally verify conditions (i) and (ii), as described in claim 1, for a pre-computed set of cryptographic parameters stored in the memory.

At least for the reasons above, claim 1 is patentable. Independent claims 12 and 19 are patentable at least because they include distinguishing features similar to those of claim 1. The remaining claims are patentable at least because of their dependencies.

At least for the reasons above, claim 1 is patentable. Independent claims 12 and 19 are patentable at least because they include distinguishing features similar to those of claim 1. Claims 2-5, 13, 15 and 16 are patentable at least because of their dependency.

Claims 6, 8-10, 14, 17 and 18 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hopkins as applied to claims 1, 3, 5 and 13, and further in view of Futa et al. (U.S. Patent No. 7,130,422 B2, hereinafter "Futa").

Claim 7 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hopkins in view of Futa as applied to claim 1, and further in view of Matyas (U.S. Patent No. 4,736,423, hereinafter "Matyas").

Claims 6-10, 14, 17 and 18 are patentable at least because Futa and Matyas do not remedy the deficiencies of the Hopkins reference.

CONCLUSION

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 9, 2010

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839
703 836 6620